Alexandria Police Department

Directive 3.2

AUTOMATED SYSTEMS

Effective Date: 03-14-2019	**Cancels**: 03-03-2009	
Updated Date:	**Section(s):**	**SME Review Date:**
Updated Date:	**Section(s):**	**2022**
Updated Date:	**Section(s):**	

CONTENTS

3.2.01 PURPOSE AND POLICY
3.2.02 DEFINITIONS
3.2.03 RESPONSIBILITIES
3.2.04 PROCUREMENT PROCEDURES
3.2.05 RECEIPT OF COMPUTER-RELATED ITEMS
3.2.06 SYSTEMS BACK-UP AND SECURITY
3.2.07 SOFTWARE DEVELOPMENT POLICY

3.2.01 PURPOSE AND POLICY

The purpose of this directive is to establish responsibilities for the acquisition, budgeting, development, training, use, and maintenance of the Department’s computer resources.

It is the policy of the Department to manage information technology efficiently and effectively in order to accomplish the Department's mission. It is the policy of the Technology, Data and Analysis Division (TDAD) to provide guidance and assistance in the acquisition, installation, training, and use of computer equipment and programs within the Department. This includes budget preparation, computer supply management, and review of purchase requests for continuous oversight of the Department's computer activities.

3.2.02 DEFINITIONS

ACA (Accurint Crime Analysis) – *Accurint Crime Analysis is a secure online dashboard that enables crime data sharing, pattern analysis, crime mapping, predictive crime analytics and reporting for law enforcement. It is a map driven automated system that allows users to query crime, calls for service, and field interviews geographically.*

AJIS - Alexandria Justice Information System. **[82.3.6; 82.3.8]**

CAD - Computer Aided Dispatch.

Community Crime Map – Public facing mapping program displaying crime information (incidents mapped at the 100 block to protect privacy). **[81.2.4]**

Hardware - Computer equipment. **[82.3.1]**

ITS – The City's Information Technology Services.

ITSC - Information Technology Steering Committee; the City's technology oversight committee. **[82.1.3; 82.2.1]**

LInX – (Law Enforcement Information Exchange) – *A nationally shared database of law enforcement data. LInX provides participating law enforcement partner agencies with secure access to regional crime and incident data and the tools needed to process it, enabling investigators to search across jurisdictional boundaries to help solve crimes and resolve suspicious events.*

PRISM – (Police Reporting and Investigative Search Module) In-house query and reporting application.

RMS - (Records Management System) *The Department's RMS is the primary software application and database that houses the large majority of departmental crime data. The RMS works in tandem with the Field Based Reporting (FBR) software used to complete and submit police reports electronically.*

Software - Computer programs.

Software license – User's agreement to operate computer programs.

Upgrade – The latest version of improved computer programs.

WebRMS - The current vendor's name for the records management software.

3.2.03 RESPONSIBILITIES

A. The TDAD commander will ensure the following tasks are accomplished.

1. Annual report preparation *in coordination with the Public Information Office*;

2. Annual TDAD budget preparation; **[17.2.2]**

3. Supervision and training of TDAD staff;

4. Develop and implement internal TDAD policies and procedures;

5. Recommend approval or disapproval, or other actions relating to the procurement or development of computer applications, equipment, programs or supplies;

6. Coordinate Department automation plans, resources and policies with ITS);

7. Designation and training of systems automation representatives and backup personnel;

8. Represent the Department at local, state and national criminal justice meetings, conferences, and seminars dealing with automation;

9. Coordinate grants that impact the automated systems of the Department;

10. Collaborate in the annual planning for future Department automation;

11. Recommend automated equipment, software, and training needed to meet Department accreditation standards;

12. In coordination with ITS and in compliance with written City standards, develop and maintain Department standards for computer-related equipment, programs, supplies, and services;

13. Recommend modifications to ITS standards via the Chief of Police, when appropriate, to more efficiently accomplish the Department's mission;

14. Conduct periodic inspections of computer-related equipment and software, where and when necessary. Discovery of an unauthorized item may result in it being removed from the system. Notification of such discovery and removal shall be forwarded to the Chief of Police. A copy of this notification will be given to the unit commander, who will then prepare a written response to the Chief of Police;

15. TDAD personnel will continuously maintain and inventory the Department’s computers and peripheral hardware;

16. Attend the City’s Information Technology Steering Committee (ITSC) to discuss Departmental projects and leverage enterprise resources as needed and available.

B. <u>Commanders will ensure that:</u>

1. Unit personnel are trained to operate computer systems under their responsibility, and substitutes are trained to operate systems when principal operators are absent;

2. All equipment, software, publications, textbooks, storage media, supplies, and other computer items that are Department property are properly maintained and accounted for and available for use by trained and authorized members of the Department;

3. Unit personnel follow the rules of all licensed computer programs and systems in use within their unit.

4. Prepare a written response to the Chief of Police, with a copy to the TDAD commander, when notified of an unauthorized computer-related item. (see section 3.2.03.A.14, above).

C. <u>All personnel will:</u>

1. Care for and protect Department computers, equipment, software, and supplies.

2. Obtain permission from the TDAD commander or designee prior to installation of any hardware or software.

3. Implement significant alterations of computer systems only in coordination with TDAD staff. This includes but is not limited to the creation of LANs or installation of additional programs, drives, or memory.

3.2.04 PROCUREMENT PROCEDURES

A. All Purchase Requests (APD-78) for computer equipment, software, training, supplies, services, or related items, regardless of cost and whether budgeted or unbudgeted, will be routed through the TDAD commander in accordance with Police Directive 1.7, Fiscal Management.

B. No employee will commit the Department to the receipt or exchange of computer services, purchases, training, computer related travel for training or demonstrations, maintenance, or product evaluations without first obtaining approval from the TDAD and Fiscal/ Management commanders. Employees making or authorizing unapproved expenditures will be held accountable for their actions and may be held financially responsible.

C. Emergency purchases requiring immediate delivery or repair due to unforeseen circumstances or to ensure public safety will be coordinated with the TDAD commander in compliance with guidelines contained in Police Directive 1.7, Fiscal Management.

D. TDAD personnel will advise commanders in the preparation of automated budget justifications. Commanders will ensure that requests for assistance are made in a timely manner to allow proper coordination prior to submission to Fiscal/Fleet Management.

E. Department-wide ideas and requests for new technologies (software and/or hardware) will be discussed collaboratively with the appropriate TDAD staff. TDAD will provide technical expertise and guidance to ensure technologies meet Department and City specifications on security, data redundancy, and storage. Attendance at the ITSC will ensure City-wide technologies and resources are utilized.

3.2.05 RECEIPT OF COMPUTER-RELATED ITEMS

A. The TDAD commander will be notified upon receipt of all computer equipment, software programs, and commencement of computer services, regardless of the cost of such items. The original or a copy of all packing receipts will be immediately forwarded to the TDAD commander.

B. All registrations, licenses, and warranty cards and forms will be completed using the following information:

Technology, Data and Analysis Commander
Alexandria Police Department
3600 Wheeler Ave
Alexandria, VA 22304
Telephone: (703) 746-6698

Under <u>no</u> circumstances will warranty or registration be made using individuals' names for products that are Department property. In addition, all items to be used to purchase future upgrades, such as title pages, are to be forwarded to TDAD for storage and future upgrade use.

C. **<u>Authorized software are those computer programs:</u>**

1. Purchased for use by ITS and APD from authorized funds or procured under any technology transfer agreement, Federal or State grants, or asset forfeiture funds;

2. Procured by individuals using personal funds and licensed, registered, or authorized to be installed on a Department computer. Proof of such permission will be personal possession of original disks, manuals, and licenses. Installation and use must comply with the manufacturer's license; and

3. Equipment, procedures, texts, or publications provided to the Department through the TDAD commander or the Chief of Police.

D. When members of the Department provide personal computer equipment for personal use with Department software or equipment, it will be clearly labeled as such.

3.2.06 SYSTEMS BACK-UP AND SECURITY

A. **The TDAD Commander** will ensure that written guidelines exist for RMS system failure. These backup guidelines will be maintained in the Department of Emergency Communications and will consist of an emergency contact list of all TDAD personnel and APD employees trained in the operations of computer systems deemed operationally imperative by the Chief of Police.

B. **The RMS administrator will:**

1. Ensure central computer systems are regularly backed up.

   a. Critical data is replicated to a redundant system at an offsite location.
   b. The redundant system is operational.
   c. Full database backups are run daily.
   d. Transaction log backups are run every fifteen minutes.

2. Ensure security of computer records. **[82.1.6]**

   a. The regular disabling of passwords will take place:

      - During routine changing of passwords as a general security precaution, or
      - When a person has left the Department’s employment.

   b. Access codes, access violations, and passwords are determined at the discretion of the system administrator.

   c. The system administrator can set how often passwords expire. This is currently done at 90 days after the password was first set.

   d. The system administrator can set the number of incorrect attempts that will be allowed before a login is disabled. This is currently set at five attempts.

e. The system administrator or designee will conduct an audit of passwords, access codes, and other security devices annually during the month of January.

3.2.07 SOFTWARE DEVELOPMENT POLICY

A. Software developed under the following conditions give exclusive ownership rights to the Department and the City:

1. Using Departmental equipment, supplies, or facilities; or

2. Developed during hours of employment; or

3. Incorporating or depending on Department information or data for development; or

4. Developed for Departmental research or development.

B. Employee written software:

1. Software written by Department employees independent of the above which is brought into the Department and used to support the Department's business gives the Department permanent right to use, but not ownership of the source code of the software.

2. Employees engaging in private profit making by representing computer software or hardware manufacturers may not participate in the evaluation of that software or hardware products for use by this Department while employed by this Department. Employees may not use Department employment to indicate or imply that this Department endorses the product(s).

By Authority Of:

Michael L. Brown
Chief of Police